

CNC

U.S. DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN
FILED
2013 FEB 26 P 4:01
JAMES L. SANTALLE
CLERK

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

Case No. 10-CR-246 (CNC)

OLEG NIKOLAENKO,

Defendant.

REDACTED PLEA AGREEMENT

The United States of America, by its attorneys, James L. Santelle, United States Attorney for the Eastern District of Wisconsin, Erica N. O'Neil and Brian J. Resler, Assistant United States Attorneys, and William A. Hall, Jr., Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, and the defendant, Oleg Nikolaenko, individually and by attorney Arkady Bukh, pursuant to Rule 11 of the Federal Rules of Criminal Procedure, enter into the following plea agreement:

CHARGES

The defendant has been charged in a two-count superseding indictment, which alleges violations of Title 18, United States Code, Sections 1030(a)(5) and 1037(a)(3). The defendant has also been charged in a one-count information, which alleges a violation of Title 18, United States Code, Sections 1030(a)(5).

The defendant has read and fully understands the charges contained in the indictment and information. He fully understands the nature and elements of the crimes with which he has been

charged, and those charges and the terms and conditions of the plea agreement have been fully explained to him by his attorney.

The defendant voluntarily agrees to waive prosecution by indictment in open court.

The defendant voluntarily agrees to plead guilty to the following count set forth in full as follows:

INFORMATION

THE GRAND JURY FURTHER CHARGES:

1. Beginning in approximately January 2007, and continuing until at least November 4, 2010, in the State and Eastern District of Wisconsin and elsewhere,

OLEG Y. NIKOLAENKO

knowingly caused the transmission of a program, information, code, and command that caused, and attempted to cause, the transmission of multiple commercial electronic mail messages.

2. As a result of such conduct, the defendant intentionally caused damage without authorization to a protected computer and caused at least \$5,000 in loss to one or more persons during a one-year period.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A), 1030(c)(4)(B), and 2.

The defendant acknowledges, understands, and agrees that he is, in fact, guilty of the offense described in paragraph 4. The parties acknowledge and understand that if this case were to proceed to trial, the government would be able to prove the facts in Attachment A beyond a reasonable doubt. The defendant admits that any facts known to him are true and correct, and that combined with the statements and opinions of others, establish his guilt beyond a reasonable doubt. This information is provided for the purpose of setting forth a factual basis for the plea of guilty. It is not a full recitation of the defendant's knowledge of, or participation in, this offense.

PENALTIES

The parties understand and agree that the offense to which the defendant will enter a plea of guilty carries the following maximum term of imprisonment and fine: ten years and \$250,000. The count also carries a mandatory special assessment of \$100, and a maximum of three years of supervised release. The parties further recognize that a restitution order may be entered by the court.

The defendant acknowledges, understands, and agrees that he has discussed the relevant statutes as well as the applicable sentencing guidelines with his attorney.

DISMISSAL OF SUPERSEDING INDICTMENT

The government agrees to move to dismiss the superseding indictment at the time of sentencing.

ELEMENTS

The parties understand and agree that in order to sustain the charge of transmitting a program, code, command, or information to a computer, intending to cause damage, as set forth in the information, the government must prove each of the following propositions beyond a reasonable doubt:

First, the defendant knowingly caused the transmission of a program, code command, or information to a computer without authorization;

Second, as a result of the transmission, the defendant intentionally impaired the integrity or availability of data, a program, a system, or information; and

Third, the computer was used in or affected interstate or foreign commerce or communication.

In order for the enhanced penalties of § 1030(c)(4)(B) to apply, the government must also prove loss to persons during a 1-year period from the defendant's course of conduct affecting a protected computer aggregating at least \$5,000 in value.

SENTENCING PROVISIONS

The parties agree to waive the time limits in Fed. R. Crim. P. 32 relating to the presentence report, including that the presentence report be disclosed not less than 35 days before the sentencing hearing, in favor of a schedule for disclosure, and the filing of any objections, to be established by the court at the change of plea hearing.

The parties acknowledge, understand, and agree that any sentence imposed by the court will be pursuant to the Sentencing Reform Act, and that the court will give due regard to the Sentencing Guidelines when sentencing the defendant.

The parties acknowledge and agree that they have discussed all of the sentencing guidelines provisions which they believe to be applicable to the offense set forth in paragraph 5. The defendant acknowledges and agrees that his attorney in turn has discussed the applicable sentencing guidelines provisions with him to the defendant's satisfaction.

The parties acknowledge and understand that prior to sentencing the United States Probation Office will conduct its own investigation of the defendant's criminal history. The parties further acknowledge and understand that, at the time the defendant enters a guilty plea, the parties may not have full and complete information regarding the defendant's criminal history. The parties acknowledge, understand, and agree that the defendant may not move to withdraw the guilty plea solely as a result of the sentencing court's determination of the defendant's criminal history.

Sentencing Guidelines Calculations

The parties acknowledge, understand, and agree that the sentencing guidelines calculations included in this agreement represent the positions of the parties on the appropriate sentence range under the sentencing guidelines. The defendant acknowledges and understands that the sentencing

guidelines recommendations contained in this agreement do not create any right to be sentenced within any particular sentence range, and that the court may impose a reasonable sentence above or below the guideline range. The parties further understand and agree that if the defendant has provided false, incomplete, or inaccurate information that affects the calculations, the government is not bound to make the recommendations contained in this agreement.

Relevant Conduct

The parties acknowledge, understand, and agree that pursuant to Sentencing Guidelines Manual § 1B1.3, the sentencing judge may consider relevant conduct in calculating the sentencing guidelines range, even if the relevant conduct is not the subject of the offense to which the defendant is pleading guilty.

Base Offense Level

The parties agree to recommend to the sentencing court that the applicable base offense level for the offense charged in the information is 6 under Sentencing Guidelines Manual § 2B1.1(a)(2).

Specific Offense Characteristics

The parties agree to recommend to the sentencing court that the following increases will apply to the base offense level:

- a. a fourteen-level increase for loss greater than \$400,000 but less than \$1,000,000 under Sentencing Guidelines Manual § 2B1.1(b)(1)(H);
- b. a six-level increase for more than 250 victims under Sentencing Guidelines Manual § 2B1.1(b)(1)(C);
- c. a two-level increase for sophisticated means under Sentencing Guidelines Manual § 2B1.1(b)(10);

- d. a four-level increase for conviction of an offense under 18 U.S.C. § 1030(a)(5)(A) under Sentencing Guidelines Manual § 2B1.1(b)(17)(A)(ii); and
- e. a two-level increase for false registration of a domain name under Sentencing Guidelines Manual § 3C1.4.

Acceptance of Responsibility

The government agrees to recommend a two-level decrease for acceptance of responsibility as authorized by Sentencing Guidelines Manual § 3E1.1(a), but only if the defendant exhibits conduct consistent with the acceptance of responsibility. In addition, if the court determines at the time of sentencing that the defendant is entitled to the two-level reduction under § 3E1.1(a), the government agrees to make a motion recommending an additional one-level decrease as authorized by Sentencing Guidelines Manual § 3E1.1(b) because the defendant timely notified authorities of his intention to enter a plea of guilty.

Sentencing Recommendations

Both parties reserve the right to provide the district court and the probation office with any and all information which might be pertinent to the sentencing process, including but not limited to any and all conduct related to the offense as well as any and all matters which might constitute aggravating or mitigating sentencing factors.

Both parties reserve the right to make any recommendation regarding any other matters not specifically addressed by this agreement.

The government agrees to recommend a sentence no greater than nine years of imprisonment.

Court's Determinations at Sentencing

The parties acknowledge, understand, and agree that neither the sentencing court nor the United States Probation Office is a party to or bound by this agreement. The United States Probation Office will make its own recommendations to the sentencing court. The sentencing court will make its own determinations regarding any and all issues relating to the imposition of sentence and may impose any sentence authorized by law up to the maximum penalties set forth in paragraph 7 above. The parties further understand that the sentencing court will be guided by the sentencing guidelines but will not be bound by the sentencing guidelines and may impose a reasonable sentence above or below the calculated guideline range.

The parties acknowledge, understand, and agree that the defendant may not move to withdraw the guilty plea solely as a result of the sentence imposed by the court.

FINANCIAL MATTERS

The defendant acknowledges and understands that any and all financial obligations imposed by the sentencing court are due and payable upon entry of the judgment of conviction. The defendant agrees not to request any delay or stay in payment of any and all financial obligations.

The defendant agrees that, during the period of any supervision (probation or supervised release) imposed by the court in this case, the defendant will provide the Financial Litigation Unit (FLU) of the United States Attorney's Office with completed financial forms which will be provided by FLU, and will provide any documentation required by those forms. The defendant will provide FLU with such completed financial forms with required documentation within the first two months of supervision, at six month intervals thereafter during supervision, and within the last six months of scheduled supervision. The defendant acknowledges and agrees that, while he is on supervision,

the Probation Department and FLU can exchange financial information pertaining to the defendant in order to facilitate collection of any fine or restitution ordered by the court as part of the sentence in this case.

At least 45 days prior to sentencing, the defendant agrees to provide the government with completed financial forms which will truthfully and completely detail his assets and income. He also agrees to provide any documentation required by those forms. The defendant agrees that, to the extent he is able, he will repatriate sufficient assets to satisfy any financial obligations imposed by the court in this case. However, inability to satisfy his financial obligations will not be considered a breach of the plea agreement.

Fine

The parties acknowledge and understand that the government may recommend to the sentencing court that a fine be imposed against the defendant.

Special Assessment

The defendant agrees to pay the special assessment in the amount of \$100 prior to or at the time of sentencing.

Restitution

The defendant agrees to pay restitution as ordered by the court. The defendant agrees to cooperate in efforts to collect the restitution obligation. The defendant understands that imposition or payment of restitution will not restrict or preclude the filing of any civil suit or administrative action.

Forfeiture

The defendant agrees that all properties listed in the information constitute the proceeds of the offense to which he is pleading guilty, or were used to facilitate such offense. The defendant agrees to the forfeiture of these properties and to the immediate entry of a preliminary order of forfeiture. The defendant agrees that he has an interest in each of the listed properties. The parties acknowledge and understand that the government reserves the right to proceed against assets not identified in this agreement.

DEFENDANT'S WAIVER OF RIGHTS

In entering this agreement, the defendant acknowledges and understands that in so doing he surrenders any claims he may have raised in any pretrial motion, as well as certain rights which include the following:

- a. If the defendant persisted in a plea of not guilty to the charges against him, he would be entitled to a speedy and public trial by a court or jury. The defendant has a right to a jury trial. However, in order that the trial be conducted by the judge sitting without a jury, the defendant, the government and the judge all must agree that the trial be conducted by the judge without a jury.
- b. If the trial is a jury trial, the jury would be composed of twelve citizens selected at random. The defendant and his attorney would have a say in who the jurors would be by removing prospective jurors for cause where actual bias or other disqualification is shown, or without cause by exercising peremptory challenges. The jury would have to agree unanimously before it could return a verdict of guilty. The court would instruct the jury that the defendant is presumed innocent until such time, if ever, as the government establishes guilt by competent evidence to the satisfaction of the jury beyond a reasonable doubt.
- c. If the trial is held by the judge without a jury, the judge would find the facts and determine, after hearing all of the evidence, whether or not he was persuaded of defendant's guilt beyond a reasonable doubt.

- d. At such trial, whether by a judge or a jury, the government would be required to present witnesses and other evidence against the defendant. The defendant would be able to confront witnesses upon whose testimony the government is relying to obtain a conviction and he would have the right to cross-examine those witnesses. In turn the defendant could, but is not obligated to, present witnesses and other evidence on his own behalf. The defendant would be entitled to compulsory process to call witnesses.
- e. At such trial, defendant would have a privilege against self-incrimination so that he could decline to testify and no inference of guilt could be drawn from his refusal to testify. If defendant desired to do so, he could testify on his own behalf.

The defendant acknowledges and understands that by pleading guilty he is waiving all the rights set forth above. The defendant further acknowledges the fact that his attorney has explained these rights to him and the consequences of his waiver of these rights. The defendant further acknowledges that as a part of the guilty plea hearing, the court may question the defendant under oath, on the record, and in the presence of counsel about the offense to which the defendant intends to plead guilty. The defendant further understands that the defendant's answers may later be used against the defendant in a prosecution for perjury or false statement.

The defendant acknowledges and understands that he will be adjudicated guilty of the offense to which he will plead guilty and thereby may be deprived of certain rights, including but not limited to the right to vote, to hold public office, to serve on a jury, to possess firearms, and to be employed by a federally insured financial institution.

The defendant knowingly and voluntarily waives all claims he may have based upon the statute of limitations, the Speedy Trial Act, and the speedy trial provisions of the Sixth Amendment relating to the charge in the information. The defendant agrees that any delay between the filing of

this agreement and the entry of the defendant's guilty plea pursuant to this agreement constitutes excludable time under the Speedy Trial Act.

Further Civil or Administrative Action

The defendant acknowledges, understands, and agrees that the defendant has discussed with his attorney and understands that nothing contained in this agreement, including any attachment, is meant to limit the rights and authority of the United States of America or any other state or local government to take further civil, administrative, or regulatory action against the defendant, including but not limited to any listing and debarment proceedings to restrict rights and opportunities of the defendant to contract with or receive assistance, loans, and benefits from United States government agencies.

MISCELLANEOUS MATTERS

The defendant knowingly and voluntarily agrees to be deported and removed from the United States following the completion of any term of imprisonment in this matter. Removal and other immigration consequences are the subject of a separate proceeding, and the defendant understands that no one, including the defendant's attorney or the sentencing court, can predict to a certainty the effect of the defendant's conviction on the defendant's immigration status. The defendant nevertheless affirms that the defendant wants to plead guilty regardless of any immigration consequences, including the potential for automatic removal from the United States.

The government agrees that, if the defendant meets the requirements for participation in the Treaty of International Prisoner Transfer or Exchange, it will not oppose his participation in this program.

GENERAL MATTERS

The parties acknowledge, understand, and agree that this agreement does not require the government to take, or not to take, any particular position in any post-conviction motion or appeal.

The parties acknowledge, understand, and agree that if the court orders that this agreement be sealed, this agreement will remain under seal and not become part of the public record in this case as specified in the court's sealing order.

The parties acknowledge, understand, and agree that the United States Attorney's office is free to notify any local, state, or federal agency of the defendant's conviction.

The defendant understands that pursuant to the Victim and Witness Protection Act, the Justice for All Act, and regulations promulgated thereto by the Attorney General of the United States, the victim of a crime may make a statement describing the impact of the offense on the victim and further may make a recommendation regarding the sentence to be imposed. The defendant acknowledges and understands that comments and recommendations by a victim may be different from those of the parties to this agreement.

The government agrees that it will not further prosecute Mr. Nikolaenko for any violations of federal law relating to the use of the Mega-D or Ozdok botnet to send spam email messages. The government agrees that it will not prosecute Mr. Nikolaenko for other violation(s) of Title 18, United States Code, Sections 371, 1028, 1028A, 1029, 1030, 1037, 1341, 1343, 1344, 1349, 1956, and 1957 involving the use of a computer, if such violation(s) were committed solely for purposes of commercial advantage or private financial gain.

Further Action by Internal Revenue Service

Nothing in this agreement shall be construed so as to limit the Internal Revenue Service in discharging its responsibilities in connection with the collection of any additional tax, interest, and penalties due from the defendant as a result of the defendant's conduct giving rise to the charges alleged in the information.

EFFECT OF DEFENDANT'S BREACH OF PLEA AGREEMENT

The defendant acknowledges and understands if he violates any term of this agreement at any time, engages in any further criminal activity prior to sentencing, or fails to appear for sentencing, this agreement shall become null and void at the discretion of the government. The defendant further acknowledges and understands that the government's agreement to dismiss any charge is conditional upon final resolution of this matter. If this plea agreement is revoked or if the defendant's conviction ultimately is overturned, then the government retains the right to reinstate any and all dismissed charges and to file any and all charges which were not filed because of this agreement. The defendant hereby knowingly and voluntarily waives any defense based on the applicable statute of limitations for any charges filed against the defendant as a result of his breach of this agreement. The defendant understands, however, that the government may elect to proceed with the guilty plea and sentencing. If the defendant and his attorney have signed a proffer letter in connection with this case, then the defendant further acknowledges and understands that he continues to be subject to the terms of the proffer letter.

VOLUNTARINESS OF DEFENDANT'S PLEA

The defendant acknowledges, understands, and agrees that he will plead guilty freely and voluntarily because he is in fact guilty. The defendant further acknowledges and agrees that no

threats, promises, representations, or other inducements have been made, nor agreements reached, other than those set forth in this agreement, to induce the defendant to plead guilty.

ACKNOWLEDGMENTS

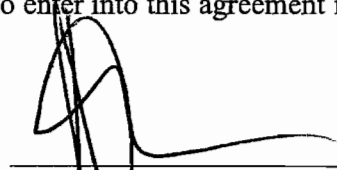
I am the defendant. I am entering into this plea agreement freely and voluntarily. I am not now on or under the influence of any drug, medication, alcohol, or other intoxicant or depressant, whether or not prescribed by a physician, which would impair my ability to understand the terms and conditions of this agreement. My attorney has reviewed every part of this agreement with me and has advised me of the implications of the sentencing guidelines. I have discussed all aspects of this case with my attorney and I am satisfied that my attorney has provided effective assistance of counsel.

Date: 6-15-12


OLEG NIKOLAENKO
Defendant


I am the defendant's attorney. I carefully have reviewed every part of this agreement with the defendant. To my knowledge, my client's decision to enter into this agreement is an informed and voluntary one.

Date: 6-15-12



ARKADY BUKH
Attorney for Defendant

For the United States of America:

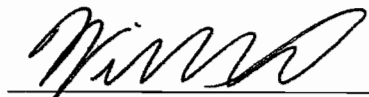
Date: 6/15/12


JAMES L. SANTELLE
United States Attorney

Date: 6/15/12


BRIAN J. RESLER
Assistant United States Attorney

Date: 6/15/12


WILLIAM A. HALL, JR.
Trial Attorney
Computer Crime & Intellectual Property
Section, U.S. Department of Justice

ATTACHMENT A

I. Affking Affiliate Program

On August 9, 2009, in federal district court for the Eastern District of Missouri, Jody M. Smith pled guilty to a one-count information charging a conspiracy to traffic in counterfeit Rolex watches. The investigation into Smith revealed, and Smith admitted in his guilty plea, that he contracted with “spammers” – senders of unsolicited commercial electronic mail messages, commonly known as “spam e-mails” – to solicit customers to purchase his counterfeit Rolexes. Smith admitted that he paid more than \$2,000,000 to the spammers to send the e-mail messages.

As part of the investigation into Smith’s case, the FBI, assisted by the FTC, determined that Smith’s enterprise, which operated both within and outside the United States, was named “Affking.” The FTC received over three million complaints regarding spam messages connected to this operation.

In his guilty plea, Smith identified Australian citizen and resident Lance Atkinson as a co-conspirator in the Affking e-mail marketing and counterfeiting operation. Based on other undercover investigations, the FBI and FTC determined that in addition to selling counterfeit Rolexes, Affking also deceptively marketed and sold counterfeit herbal “male enhancement” pills and generic prescription drugs that were falsely advertised as FDA-approved.

As part of the ongoing investigation into Smith, Atkinson, and Affking, the United States government sought assistance from Australian and New Zealand authorities. On December 23, 2008, Lance Atkinson was interviewed by the Australian Communications and Media Authority. The purpose of the interview was to get the details of Atkinson’s and Smith’s spam enterprise. In the interview, Atkinson explained his involvement in the Affking and related enterprises, including Affking predecessor companies Genbucks and Sancash. Atkinson admitted that, using a nickname, he posted messages on a pro-spam Internet bulletin boards seeking spammers to promote the herbal pills. Atkinson recalled that his largest spamming affiliates were Russian. Specifically, he recalled that two of his largest Russian spamming affiliates used the online monikers “Docent” and “Dem.” Atkinson also admitted that he also used banner advertisements on website and advertisements placed within internet search engines to market the products. Atkinson estimated that 80% of all of the advertising was done by the affiliates via spam e-mails, with the other 20% done through banner and internet search engine advertisements.

As part of its investigation, the FTC obtained chat logs which were seized during a search warrant executed in New Zealand at Lance Atkinson’s brother’s house. One chat log was a conversation between Lance Atkinson’s brother, Shane Atkinson, and “Docent” in January 2007. The chat, in pertinent part, reflected that “Docent” was interested in sending additional spam messages on Lance Atkinson’s behalf. In the chat, Shane Atkinson indicated that he would have Lance Atkinson get in touch with “Docent” soon.

According to the FTC investigation, Lance Atkinson controlled an ePassporte online digital currency account in the name of New Pacific Resources, a company registered in the British Virgin

Islands. Between October 2006 and December 2007, Atkinson's ePassporte account received over \$1.7 million from Genbucks, the Smith/Atkinson company affiliated with Affking which also sold herbal diet pills, male enhancement pills, and as counterfeit watches. This account transferred over \$1.8 million to other accounts as commissions.

Lance Atkinson recalled during his interview that "Docent," the Russian affiliate spammer, used an ePassporte account under the name of "Genbucks_dcent." On November 19, 2009, the FBI received records from ePassporte. The ePassporte account "Genbucks_dcent" was registered in the name of Oleg Nikolaenko, residing at xx/xx Spasskiy Proezd, Vidnoe x, Russian Federation, e-mail addresses: ddarwinn@gmail.com and 4docent@gmail.com, telephone number 792658xxxxx. Lance Atkinson's ePassporte account made numerous payments to Nikolaenko's "Genbucks_dcent" ePassporte account, including payments totaling \$464,967.12 between June 6, 2007, and December 14, 2007.

II. Botnet

The Director of Malware Research at Secure Works, a computer security company, determined that many of the spam e-mail messages touting Affking products were routed without authorization through a vast number of compromised computers, a computer network usually referred to as a "botnet." In early 2008, the director identified one botnet, which he named "Mega-D," as one which sent spam promoting Affking's products. The director determined that Mega-D was the largest botnet in the world at that time, accounting for approximately 32% of all spam. The director estimated that the botnet was capable of sending ten billion spam e-mail messages a day, all of which contained materially falsified header information. The sending of this amount of spam was harmful to the infected computers themselves, as it impaired the computers' ability to function at legitimate tasks, and harmful to internet service providers, as it required significant internet bandwidth to send these e-mails. According to internet service providers and network security providers, the security, storage, and network degradation costs incurred as a result of the Mega-D botnet exceeded tens of thousands of dollars.

On November 2, 2009, the FBI obtained a copy of an e-mail which was sent by the Mega-D botnet. This e-mail was provided to the FBI by the Director of Malware Research at Secure Works. A review of the e-mail header reflected that it contained materially false information, in that the sender and recipient both appear to be yamamoto.kenichiro@somec.co.jp, when in fact the true sender information revealed that the true sender of the e-mail was e-mail jnaka@4dcsi.com. This materially false header information made the e-mail appear as if the recipient sent the e-mail to him or herself, when in fact the e-mail came from an entirely different e-mail account.

The Mega-D botnet was controlled by centralized computers, known as command-and-control servers, that processed requests and delivered data to the infected computers. The domain names of these command-and-control servers were not registered to any individuals affiliated with the Affking affiliate program. Rather, the domain names for the servers were fictitiously registered

to various purported individuals worldwide, including in the United States, France, Germany, Poland, Russia, Sweden, the Netherlands, and Ukraine.

II. E-mail

On November 24, 2009, the FBI received subscriber records for the e-mail account ddarwinn@gmail.com from Google. The records revealed that the ddarwinn@gmail.com account was registered to Oleg Nikolaenko, residing at xx/xx Spasskiy Pr, Vidnoe x, Moscow, Russia, telephone number 792658xxxxx.

Search warrants were obtained for e-mail accounts ddarwinn@gmail.com and 4docent@gmail.com on July 29, 2010, and October 29, 2010. The 4docent@gmail.com account contained e-mails from Nikolaenko to others, including Affking1@gmail.com, an e-mail address belonging to Lance Atkinson. These e-mails corroborated the business relationship between Nikolaenko and Lance Atkinson, including copies of sample spam messages, references to sending large numbers of e-mails selling purported male enhancement products, and transfers of money to Nikolaenko's account.

The 4docent@gmail.com account also contained numerous executable files which were analyzed by the Director of Malware Research at Secure Works. In the director's expert opinion, copies of the executable files found in the 4docent@gmail.com are samples of the malware family known as Mega-D, which was used to infect computers worldwide to make them part of the Mega-D botnet.

III. FireEye crippling the Mega-D botnet

Computer network security company FireEye reports that it crippled the Mega-D botnet on November 4, 2009, by convincing U.S.-based internet service providers to shut down Mega-D's command-and-control computers and to redirect the infected computers, known as bots, looking for a command-and-control computer to so-called sinkholes, which collected information about the botnet, but did not send out any further commands to the infected computers. By doing so, FireEye reports that it reduced the spam sent by the Mega-D botnet from 11.8 percent of all spam sent worldwide on November 1, 2009, to less than 0.1 percent on November 4, 2009.

Based on information obtained through these sinkholes, FireEye was able to identify approximately 509,000 computers infected with the malware which causes computers to become bots seeking direction from the Mega-D command and control computers. An analysis of this data revealed that approximately 136 of the infected computers' IP addresses resolved to addresses in the State of Wisconsin, including many in the Eastern District of Wisconsin. According to the Director of Malware Research at Secure Works, when these infected computers were functioning as part of the botnet, a substantial number would have sent spam e-mail messages out in interstate and foreign commerce advertising the Affking products.

M86 Security, the largest provider of secure web gateways and the largest independent provider of web and e-mail content security in the world, reported that by November 9, 2009, the spam from the Mega-D botnet had stopped altogether. However, it also reported that the botnet bounced back, with spam sent by it exceeding pre-takedown levels by November 22, 2009, and constituting 17% of worldwide spam by December 13, 2009.

IV. Travel by the defendant

Defendant Oleg Yegorovich Nikolaenko, date of birth July xx, 19xx, residing at xx/xx Spasskiy Proezd, Vidnoe x, Russian Federation, e-mail address ddarwinn@gmail.com, telephone number 792658xxx, applied for visitor's visa to enter the United States on June 18, 2009. Nikolaenko entered the United States in Los Angeles on July 17, 2009, and left on July 27, 2009, according to U.S. government and airline records.

Travel records revealed that Nikolaenko again entered the United States in New York on October 29, 2009, and left from Los Angeles on November 9, 2009. According to hotel records, Nikolaenko visited Las Vegas, Nevada, from November 2, 2009, to November 6, 2009. According to information obtained from Google, on the day that Nikolaenko left the United States, November 9, 2009, the e-mail accounts ddarwinn@gmail.com and 4docent@gmail.com were logged into from IP address 65.86.127.226, which is registered to The Tower Hotel, Beverly Hills, California.

On October 30, 2010, Nikolaenko again entered the United States at the port of entry located at JFK airport in New York. Records indicated that he was staying at the Bellagio hotel in Las Vegas, Nevada for the Specialty Equipment Market Association ("SEMA") car show. Pursuant to a complaint and arrest warrant, Nikolaenko was arrested in his hotel room on November 4, 2010, and a notebook computer was seized.

V. Defendant's computer

A forensic analysis of the laptop computer seized when the defendant was arrested revealed that the defendant had saved his computer chats with Lance and Shane Atkinson. These chats corroborated the business relationship between them. According to the chats and other information recovered from the computer, Nikolaenko registered false internet domain names to assist in marketing the Affking products, created spam messages which were sent using the Mega-D botnet, and assisted in recruiting others to send spam on behalf of Affking. The defendant's laptop also had a control script, which was used to control the Mega-D botnet. The laptop also contained an Affking spreadsheet, which listed many known Affking affiliates and money that had been paid to them, including to Nikolaenko himself.

The defendant now admits that he was one of the individuals who controlled the Mega-D botnet, causing it to send out spam messages on behalf of Affking and other affiliate networks and that, as a result of this spamming activity, he received in excess of \$400,000.